REMARKS

Applicant hereby responds to the Office Action dated June 17, 2004 within the shortened three month statutory period for response. The Examiner rejects claims 1-23 and Applicant thanks the Examiner for the detailed responses to Applicant's previous arguments. Upon entry of the foregoing amendments, Applicant adds claims 24-28, so claims 1- 28 are now pending in the application. Support for the various amendments may be found in the originally filed specification, claims, and figures. No new matter has been introduced by these amendments. Reconsideration of this application is respectfully requested.

The Examiner states that the drawings are informal and are acceptable for examination, but formal drawings will be required when the application is allowed. Applicant shall submit formal drawings upon allowance of the application.

The Examiner rejects claims 1-3, 8-9, 13-16, and 20 under 35 USC 103(a) as being unpatentable over Atkinson et al US Patent No 5,892,904 in view of Berstis et al US Patent No 6,735,694. Applicant respectfully traverses these rejections. With regard to claims 1 and 14, the Examiner asserts that Atkinson fails to teach the formatting of data occurring in real time, however that Berstis teaches that upon retrieving the data, formatting of the retrieved data occurs in real time. Berstis is directed toward certifying the authenticity of a webpage copy. Berstis discloses a method of copying a webpage at a client computer, applying a mathematical transform to the copy and concatenating a mathematical transform to identifying information in order to generate a signature. However, the Berstis process includes the certification attached to the webpage copy at the client computer. For example, Berstis discloses "The user desires to 'prove' or 'validate' his or her 'copy' at some later time or upon a given occurrence. To this end, a 'certified' copy is generated at the client machine." (column 2, lines 8-11, emphasis added). (See

also Berstis Figure 5). Berstis later transmits a signature stream, that was used to certify the webpage copy, to a server. However, the server only verifies that the signature stream is valid before adding it to a database. Berstis only discloses providing an authentication to a webpage copy to demonstrate that a webpage was copied at a certain time and/or by a certain user. According to Berstis, third-parties may later access a signature database to verify that a user copied a webpage at a given time. However, Berstis fails to disclose a means for adding a signature or certification to a webpage at a server, prior to feeding the webpage to a client. The absence of this step in Berstis is critical, because it does not lead to certification of the webpage source. It can be assumed that according to the teachings of Berstis, a counterfeit webpage copy could just as easily be certified as a legitimate webpage. As such, Berstis does not disclose or suggest "upon retrieving the data, formatting the retrieved data in real-time at said server, wherein the formatted data includes at least one authenticity key " as required by amended independent claims 1, 14 and 24.

With regard to claims 8 and 13, the Examiner asserts that the step of "said server being configured to insert an authenticity key into the web page requested from said client" is taught by Berstis. Berstis may disclose adding a certification to a webpage copy, however as set forth above, Berstis teaches the insertion of a certification at the client computer. As such, Berstis does not disclose or suggest a certification or signature process occurring prior to sending a webpage to a client.

The Examiner also rejects claims 2- 7, 9-12 and 15-23 which variously depend from independent claims 1, 8, 13 and 14. The Examiner additionally rejects claims 4, 6, 10-11, 17 and 23 under 35 USC 103(a) as being unpatentable over Atkinson et al US Patent No 5,892,904 in view of Berstis et al US Patent No 6,735,694 and further in view of Wallent (6,366,912).

Applicant respectfully traverses these rejections. Applicant asserts that dependent claims 2-7, 9-12 and 15-23 are differentiated from the cited prior art for at least the same reasons as set forth above for differentiating independent claims 1, 8, 13 and 14 from the prior art.

Regarding the Examiner's Response to Arguments, beginning on page 3, the Examiner maintains that Atkinson teaches the step of inserting an authenticity key into the data requested from the client thereby facilitating the client to authenticate the authenticity key to verify the source of the data. Thus, according to the Examiner, Atkinson teaches all of the functionality of the authentication server. However, Atkinson discloses an authenticity key which is inserted into a code element prior to making the element available for transfer across a network. In other words, once a signature is attached to a data element, a security server does not re-sign the data element unless it is modified in any way. Atkinson does not disclose or suggest the insertion of an authenticity key or signature which is inserted into a data element prior to each request for the data element. As such, Atkinson does not disclose or teach the step of "said server being configured to insert an authenticity key in real time" as disclosed in currently amended claims 8, 13 and 24, and previously amended claims 1 and 14.

None of the cited references disclose a means for determining whether or not a data element requires authentication. While Atkinson generally discloses a browser application determining if a code element contains a signature, this is not the same determination step as disclosed in new independent claim 24. As such, neither Atkinson nor the other cited references disclose or suggest the step of "determining if said data includes a code which requires said data to be authenticated", as required by new independent claim 24.

Further, the cited references do not disclose a means for decrypting a preferences key using a master preferences key and decrypting a preferences file using the decrypted preferences

key in order to obtain preferences indicia regarding what type of visual signature to add to authenticated data. As such, the cited references do not disclose or suggest adding a visual signature to authenticated data through the steps of decrypting a preferences key, decrypting a preferences file using the preferences key, obtaining instruction from the preferences file and inserting a visual signature into said data based on preference file instructions as is disclosed in new dependent claims 25 - 28.

In view of the above remarks and amendments, Applicant respectfully submits that all pending claims properly set forth that which Applicant regards as its invention and are allowable over the cited prior art. Accordingly, Applicant respectfully requests allowance of the pending claims. The Examiner is invited to telephone the undersigned at the Examiner's convenience, if that would help further prosecution of the subject Application. Applicant authorizes and respectfully requests that any fees due be charged to Deposit Account No. 19-2814.

Respectfully submitted,

Dated: August 13, 2004

Howard Sobelman
Reg. No. 39,038

SNELL & WILMER L.L.P.
400 E. Van Buren
One Arizona Center ·
Phoenix, Arizona 85004
Phone: 602-382-6228
Fax: 602-382-6070
Email: hsobelman@swlaw.com